REMARKS

The Office Action dated March 15, 2006 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 8, 21, 25-27, 29, and 31 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 11 and 12 have been canceled without prejudice or disclaimer. No new matter has been added. Claims 1-3, 5-10, 13-15, 17-19, 21-27, and 29-33 are currently pending in the application and are respectfully submitted for consideration.

The Office Action objected to claims 8, 25, 26, 27, and 31 due to certain informalities. These claims have been amended to correct the noted informalities. Therefore, Applicants submit that the objection to the claims is rendered moot.

Claims 3, 8, 21-22, 29, and 31 were rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention.

With respect to claim 3, the Office Action states that the recitation of "said encryption module further comprises a public key encryption module" is redundant because claim 1 already recites a public key module in communication with said encryption module. Applicants respectfully traverse this rejection because claim 1 does not recite a "public key encryption module." Rather, claim 1 merely recites a public key module for storing a public key. As illustrated in figures 3 and 4, certain embodiments of the present invention include both a public key module and a public key encryption module. Consequently, Applicants respectfully request that the rejection of claim 3 be withdrawn.

With respect to claim 8, the Office Action takes the position that the recitation of "said apparatus further comprising a bonding option circuit" is redundant because claims 6 and 7 already recite a bonding option circuit. Applicants respectfully traverse this rejection because neither claim 6 nor claim 7 recites a "bonding option circuit." Rather, claims 6 and 7 recite a "bonding option output." As such, the recitation of a "bonding option circuit" in claim 8 is not redundant. Therefore, Applicants respectfully request that the rejection of claim 8 be withdrawn.

With respect to claim 21, the Office Action states that the recitation of "the comparator" lacks antecedent basis. Claim 21 has been amended to recite "said comparing device" instead of "the comparator." Thus, the rejection of claim 21 is rendered moot.

With respect to claim 29, the Office Action states that the recitation of "determining if the first bit string matched the second bit string" should instead recite "determining if the first bit string matched the third bit string." Claim 29 has been amended to reflect this change. Therefore, the rejection of claim 29 is rendered moot.

With respect to claim 31, the Office Action states that "said determining a final output step" lacks antecedent basis. Therefore, claim 31 has been amended to recite "said determining a final output enable signal step." As such, Applicants submit that the rejection of claim 31 is rendered moot.

In the Office Action, claims 1-3, 5-15, 17-19, and 21-24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello (U.S. Patent No. 6,463,537) in view of Weiss (U.S. Patent No. 6,065,029) in further view of Angelo (U.S. Patent No. 6,370,649). The Office Action takes the position that Tello discloses all of the elements of the claims, with the exception of "wherein said random number generating module comprises a linear feedback shift register and a ring oscillator in communication with said hash function module, the linear feedback shift register being configured to output a random number," and "said host being configured to receive a guess passcode from a manufacturer of the component." The Office Action cites Weiss and Angelo as allegedly disclosing the respective element of the claims. The rejection is respectfully traversed for the following reasons.

Claim 1, upon which claims 2-3 and 5-14 are dependent, recites an apparatus for enabling the functionality of a component. The apparatus includes a random number generating module for generating a random number, and a hash function module in communication with the random number generating module. The random number generating module includes a linear feedback shift register and a ring oscillator in communication with the hash function module, the linear feedback shift register being configured to output a random number. The apparatus further includes a host in communication with the random number generating module, at least one memory in communication with the host, an encryption module in communication with the memory, and a comparing device in communication with the encryption module and the hash function module. The comparing device compares a first bit string to a second bit string in order to generate a function enable output for the component. The at least one memory further comprises a guess register in communication with the host and the encryption module, the guess register being configured to receive a guess passcode from the host, and a public key module in communication with the encryption module, the public key module being configured to store a public key therein. The host is configured to receive a guess passcode from the manufacturer of the component.

Claim 15, upon which claims 17-19 and 21-24 are dependent, recites a component for selectively enabling a functionality of an electronic device. The component includes a means for generating a random bit string, a hash function module in communication with the means for generating, a means for acquiring a guess passcode in communication with the means for generating, an encryption module in communication with the means for acquiring, and a comparing device in communication with the encryption module and the hash function module. The means for generating includes a random number generating module configured to receive an initiate signal and output a random number, and a linear feedback shift register, having an input and an output, and a ring oscillator. The comparing device has an output for transmitting a functionality enable signal therefrom. The encryption module further comprises a public key encryption module, and a public key module in communication with the public key encryption module. The public key encryption module is configured to receive a public key from the public key module and a guess passcode from the means for acquiring, and generate a ciphertext bit string therefrom. The means for acquiring the guess passcode is configured to acquire the guess passcode from the manufacturer of the electronic device.

The prior art has failed to produce enablement methods that are effective against reasonably sophisticated attackers. The claimed invention resolves the limitations of the prior art by providing, in one example, a cryptographic method wherein the secure portions of the method are implemented in electronic or computer products. More specifically, embodiments of the claimed invention implement cryptographic functions for enabling functionality of electronic/computer related components, wherein the relevant secure key related information is contained within computer hardware in a non-volatile memory device and not within a purely software driven configuration. The claimed invention also provides the ability to conduct secure functionality enablement on electronic/computer related components, wherein a public key for enabling the component is contained onboard and utilized in conjunction with a randomly generated component identifier in order to selectively enable additional functionality of the component.

As will be discussed below, Tello, Weiss and Angelo, whether viewed singly or combined, fail to disclose or suggest the elements of the claims, and therefore fails to provide the advantages discussed above.

Tello discloses a modified computer motherboard security and identification system. More specifically, Tello discloses a modified motherboard with a microprocessor based security engine, enabling and disabling circuits, memory buffer circuits, modified BIOS, modified DDL, and a smart card reader and smart cards. Upon startup of the computer, the modified BIOS takes control and allows the security engine microprocessor to look for and read from a smart card in the smart card reader that is connected to the security engine microprocessor. A unique hash number is placed in the smart card during the initial set up of the security system and a complimentary hash number is assigned to the security engine memory. During startup, a software program in the flash memory of the security engine compares the hash numbers in the smart card and the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed.

Weiss discloses a method and system for providing a random number. The method includes providing an oscillator, a sampler and a sample control. The sampler is coupled to the oscillator in order to provide at least a portion of the random number. The sample control is coupled to the sampler and controls the sampler to sample the oscillator at an interval which is based on a portion of a previous random number provided using the oscillator.

Angelo discloses a computer system with a self-modifying "fail-safe" password system that allows a manufacturer to securely supply a single-use password to users who lose or misplace a system password. The fail-safe password system utilizes a fail-safe counter, an encryption/decryption algorithm, a manufacturer's public key, and a secure non-volatile memory space. Each time a fail-safe password is entered into the computer system, an application decrypts the fail-safe password and compares the resulting value, which is a hash code, to an internal hash value and increments the fail-safe counter or modifies the seed value when the hashes match. When the fail-safe counter is incremented, the previous fail-safe password is no longer valid.

Applicants respectfully submit that Tello, Weiss and Angelo, whether viewed individually or combined, fail to disclose or suggest all of the elements of the presently pending claims. For example, the cited references fail to disclose or suggest "wherein said comparing device compares a first bit string to a second bit string to generate a function enable output for the component, and wherein the first bit string comprises a ciphertext bit string generated by the encryption module and the second bit string comprises a hash value generated by the hash function module," as recited in claim 1. The Office Action takes the position that Tello discloses comparing a first bit string to a second bit string to generate a function enable output (Office Action, page 6, lines 8-10). Applicants respectfully disagree.

Tello merely discloses that a software program in the flash memory of the security engine compares a hash number in the smart card with a hash number in the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed (Tello, Column 5, lines 21-35). Tello does not disclose or suggest comparing a cipher text bit string generated by an encryption module with a hash value generated by a hash function module and generating a function enable output based on the comparison, as recited in claim 1. Wiess and Angelo also fail to cure this deficiency in Tello.

According to certain embodiments of the present invention, an identification module 28 is used to store a component identification number. The component identification number is transmitted from identification module 28 to hash function module 29. The hash function module 29 is configured to receive the pre-image input from identification module 28 and output a hash value. The hash value generated by hash function module 29 is transmitted to comparator 20 as a second input 20b. Further, host 18 obtains a guess passcode from the manufacturer and transmits the guess passcode to guess register 19. The guess passcode is then transmitted as clear text to public key encryption module 35 (Specification, page 23, lines 9-23 and Fig. 3).

Additionally, as discussed in the present specification, public key module 34, which contains the public key for the device, transmits the public key to public key encryption module 35. Therefore, public key encryption module 35 receives both the guess passcode and the public key as clear text inputs. These two inputs are processed/encrypted by public key encryption module 35 to generate cipher text at the output thereof. This cipher text is transmitted to the first input 20a of comparator 20. Comparator 20 then compares the cipher text received from the public key encryption module 35 representing the guess passcode with the hash value generated by the hash function module representing the identification number of the component. If the comparator 20 determines that these two values match, then an enable signal is output from comparator 20 indicating that the device 33 has determined that the guess passcode is authentic and that the corresponding functionality of the component should be enabled (Specification, page 24, lines 1-20 and Fig. 3).

Applicants respectfully submit that Tello, Weiss and Angelo fail to disclose or suggest the above-discussed configuration. Therefore, the combination of references fail to disclose or suggest "wherein said comparing device compares a first bit string to a second bit string to generate a function enable output for the component, and wherein the first bit string comprises a ciphertext bit string generated by the encryption module and the second bit string comprises a hash value generated by the hash function module," as recited in claim 1. Accordingly, Applicants respectfully request that the rejection of claim 1 be withdrawn.

Claims 2, 3, 5-10, and 13-14 are dependent upon claim 1. As such, claims 2, 3, 5-10, and 13-14 should be allowed for at least their dependence upon claim 1 and for the specific limitations recited therein.

Furthermore, Applicants respectfully submit that the combination of Tello, Weiss and Angelo fails to disclose or suggest all of the elements of claim 15. For instance, the cited references do not disclose or suggest "wherein said public key encryption module is configured to receive a public key from said public key module and a guess passcode from said means for acquiring, and generate a ciphertext bit string therefrom," as recited in claim 15.

As discussed above, according to certain embodiments of the claimed invention, a host 18 obtains a guess passcode from the manufacturer and transmits the guess passcode to guess register 19. The guess passcode is then transmitted as clear text to public key encryption module 35 (Specification, page 23, lines 9-23 and Fig. 3). Additionally, public key module 34, which contains the public key for the device, transmits the public key to public key encryption module 35. Therefore, public key encryption module 35 receives both the guess passcode and the public key as clear text inputs. These two inputs are processed/encrypted by public key encryption module 35 to generate cipher text at the output thereof. This cipher text is transmitted to the first input 20a of comparator 20. Comparator 20 then compares the cipher text received from the public key encryption module 35 representing the guess passcode with the hash value generated by the hash function module representing the identification number of the component. If the comparator 20 determines that these two values match, then an enable signal is output from comparator 20 indicating that the device 33 has determined that the guess passcode is authentic and that the corresponding functionality of the component should be enabled (Specification, page 24, lines 1-20 and Fig. 3).

The Office Action appears to take the position that Tello discloses "wherein said public key encryption module is configured to receive a public key from said public key module and a guess passcode from said means for acquiring, and generate a ciphertext bit string therefrom," as recited in claim 15. However, Tello only discloses that the data is encrypted by the smart card before it is sent to the security engine and then the encrypted code number is read from the register of the inserted smart card and decrypted by the security engine microprocessor using the public encryption key (Tello, Column 24, lines 17-25 and lines 46-50). Tello makes no mention of a public key encryption module that is configured to receive a public key and a guess passcode, and then generate a ciphertext bit string therefrom. Wiess and Angelo also fail to disclose or suggest such a feature. Consequently, the combination of Tello, Weiss and Angelo fails to disclose or suggest at least this element of the claims.

Therefore, Applicants respectfully request that the rejection of claim 15 be withdrawn. Claims 17-19 and 21-24 are dependent upon claim 15. As such, claims 17-19 and 21-24 should be allowed for at least their dependence upon claim 15 and for the specific limitations recited therein.

Claims 25-27 and 29-33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Davis (U.S. Patent No. 5,577,121) in view of Tello and Weiss and further in view of Angelo. The rejection is respectfully traversed for the reasons which follow.

Claim 25, upon which claims 26-27 and 29-33 are dependent, recites a method for enabling functionality of an electronic component. The method includes the steps of generating a random number, calculating a first bit string from the random number, determining a second bit string corresponding to the random number, encrypting the second bit string with a public key to generate a third bit string, comparing the third bit string to the first bit string to determine a match, and outputting a function enable signal in accordance with the comparison. The step of generating a random number includes receiving an initiate signal at a random number generating module and outputting a random number, wherein the random number generating module includes a linear feedback shift register and a ring oscillator. The encrypting step further comprises the steps of receiving a guess passcode from a host, receiving a public key, and encrypting the guess passcode and the public key to generate a ciphertext bit string. The step of determining the second bit string comprises receiving the second bit string from the manufacturer of the electronic component.

Tello, Weiss, and Angelo are discussed above. Davis discloses a transaction system for integrated circuit cards, and more specifically it discloses a method of conducting a transaction between an integrated circuit (IC) card and a transaction terminal which includes a security module. The method includes establishing communication between the terminal and the IC card and separately generating a session key in the IC card using data stored in the IC card and a code associated with the particular IC card and in the security module using data stored in the security module and the code associated with the particular IC card. The session key generated by the IC card is used to encrypt data using an encryption algorithm to obtain a first result and the session key generated by the security module is used to encrypt the same data using the same encryption algorithm to obtain a second result. The first and second results are compared and the terminal will conduct the transaction only if the comparison establishes that the first result and the second result are identical.

Applicants respectfully submit that Davis, Tello, Weiss and Angelo, whether viewed singly or combined, fail to disclose or suggest all of the elements of claim 25. For example, the cited references fail to disclose or suggest "encrypting the guess passcode and the public key to generate a ciphertext bit string," as recited in claim 25. The Office Action appears to take the position that Tello discloses this element of the claims. However, Tello, as discussed above, only discloses that the data is encrypted by the smart card before it is sent to the security engine and then the encrypted code number is read from the register of the inserted smart card and decrypted by the security engine microprocessor using the public encryption key (Tello, Column 24, lines 17-25 and lines 46-50). Tello does not disclose or suggest "encrypting the guess passcode and the public key to generate a ciphertext bit string," as recited in claim 25. Davis, Weiss and Angelo also fail to disclose this element of the claims.

In addition, the cited references do not disclose or suggest determining a second bit string corresponding to the random number, as recited in claim 25. The Office Action cites Davis as allegedly disclosing this element of the claim. Applicants submit that Davis does not determine a second bit string which corresponds to the random number. Rather, according to Davis, the security module generates a random number and sends it to the SVC. The SVC encrypts the random number with the SVC session key. The security module encrypts the random number with the security module session key (Davis, Column 13, lines 6-52). Therefore, Davis only discloses generating a random number which is then encrypted by the SVC and security module. Davis does not disclose that a second bit string corresponding to the random number is determined.

Therefore, Davis, Tello, Weiss and Angelo, whether considered singly or combined, fail to disclose or suggest all of the elements of claim 25. As such, Applicants respectfully request that the rejection of claim 25 be withdrawn.

It is also respectfully submitted that claims 26-27 and 29-33 are dependent upon claim 25 and therefore should be allowed for at least their dependence on claim 25, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art references fail to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unobvious. It is therefore requested that all of claims 1-3, 5-10, 13-15, 17-19, 21-27, and 29-33 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:jf